Universidade de Brasília
Instituto de Relações Internacionais
Programa de Pós-Graduação em Relações Internacionais
XX Curso de Especialização em Relações Internacionais

Segurança Cibernética e a Política Internacional Contemporânea: novos desafios e oportunidades

Felipe Sousa Mesquita

Artigo apresentado como requisito parcial para obtenção do título de Especialista em Relações Internacionais

s Becard, PhD

Brasília-DF

2019

RESUMO:

A vida humana está cada vez mais dependente do espaço cibernético, em virtude da progressiva evolução de novas tecnologias desde o final do século XX. Da mesma maneira em que está onipresente na vida dos indivíduos, o ciberespaço também é, hoje em dia, parte da dinâmica em que se inserem os Estados e os demais atores da sociedade internacional. Apesar de existirem outras variantes desse tema, esta pesquisa abordará aquela relacionada à segurança internacional. Seu objetivo é compreender de que forma a emergência da importância da segurança cibernética na agenda internacional impacta as relações internacionais. Trata-se de uma pesquisa qualitativa, bibliográfica e de caráter exploratório, com vistas a reunir e debater argumentos de diferentes autores e a garantir aos leitores maior familiaridade com o tema. Como forma de atingir seu objetivo, a pesquisa seguirá a seguinte estrutura: contextualização da segurança cibernética; discussão sobre o conceito de ciberespaço; definição dos atores envolvidos; características e dinâmica do *cyberwarfare* e do poder cibernético; análise dos desafios enfrentados; exposição e análise do histórico e de casos paradigmáticos. A pesquisa verificou que os temas cibernéticos adicionaram desafios inéditos para a atuação estatal, principalmente; entretanto, também criou oportunidades únicas para as estratégias governamentais para a atuação nos âmbitos externo e doméstico. Ademais, a segurança cibernética adicionou e proporcionou expressiva autonomia e importância a atores não totalmente contemplados em teorias tradicionais das relações internacionais. A maneira tradicional de conduzir os conflitos também se tornou obsoleta quando ocorrem conflitos no ciberespaço. Além disso, analisando o histórico e os casos principais, nota-se a ampliação do escopo e da complexidade dos ataques perpetrados recentemente, mostrando uma tendência de fortalecimento do tema da segurança cibernética na agenda da sociedade internacional.

Palavras-chave: Segurança cibernética; Ciberespaço; Relações Internacionais.

ABSTRACT:

Human life is increasingly dependent on cyberspace, due to the progressive evolution of new technologies, since the end of the 20th century. In addition to its ubiquitous presence in the lives of individuals, cyberspace is currently also part of the dynamics in which States and other actors of the international society are inserted. Although there are other variants of this theme, this research will address that related to international security. Its purpose is to understand how the emergence of the importance of cybersecurity on the international agenda impacts international relations. It is a qualitative, bibliographical and exploratory research, aiming to gather and debate arguments of different authors. As a way to achieve its objective, the research will follow the following structure: contextualization of cyber security; discussion on the concept of cyberspace; definition of the actors involved; characteristics and dynamics of cyberwarfare and cyberpower; analysis of existing challenges; exhibition and analysis of the history of past attacks and paradigmatic cases. The research verified that the cybernetic themes added unprecedented challenges for the state action; however, has also created unique opportunities for government strategies for external and domestic politics. In addition, cyber security added and provided significant autonomy and importance to actors not fully contemplated in traditional theories of international relations. The traditional way of conducting conflicts has also become obsolete when conflicts in cyberspace occur. Moreover, analyzing the history and main cases, one can note the broadening of the scope and complexity of recent attacks, showing a tendency to strengthen the theme of cyber security in the agenda of international society.

Keywords : Cybersecurity ; Cyberspace ; International Relations

1. Introdução

Desde o final do século XX, a política internacional tem testemunhado a emergência e o desenvolvimento de um fator com impacto substancial em sua dinâmica: as novas tecnologias digitais. Novos nomes e conceitos passaram a fazer parte do cotidiano de indivíduos, de governos e de outras organizações não governamentais, como neutralidade das redes, governança da Internet, inteligência artificial, Internet das Coisas, e Quarta Revolução Industrial. Contudo, todos esses temas estão, de alguma maneira, interligados a um, que os une e, em certa medida, os abriga: o ciberespaço, que se desdobra, na sociedade internacional, na cibersegurança. Diferentemente da política internacional tradicional, calcada na interação entre governos estatais e outros atores do sistema internacional, com regras relativamente delimitadas e certa previsibilidade, a política internacional no ciberespaço é um terreno inédito, com dinâmica particular. Por esse motivo, o tema tem sido frequentemente objeto de debates, por exemplo, em instâncias multilaterais, como no Fórum Econômico Mundial, na União Europeia e nas Nações Unidas.

Nos últimos anos, com o avanço e o aperfeiçoamento tecnológico, o ciberespaço tem abrangido, cada vez mais, processos e dados fundamentais para as mais diversas searas: administração governamental, economia global, armazenamento e disponibilidade de dados, controle de infraestrutura estratégica, segurança energética, entre outros. Essa ubiquidade das tecnologias cibernéticas no cotidiano dos indivíduos, dos governos e das empresas privadas traz consigo, apesar do grande avanço que o espaço cibernético possibilita, um grande número de vulnerabilidades, as quais serão objeto de análise deste trabalho. E são essas vulnerabilidades, como a extrema dependência das tecnologias digitais para o gerenciamento de infraestruturas e para a comunicação, um ponto fundamental para a segurança cibernética.

Ataques cibernéticos podem se originar tanto em Estados nacionais quanto em grupos não estatais, o que torna essas agressões de difícil atribuição, aumentando a incerteza em relação a elas. Ademais, esses ataques não respeitam fronteiras nem distâncias e possuem custos relativamente baixos se comparados com estratégias militares tradicionais, desestabilizando o jogo convencional de segurança e de defesa

internacionais, onde os Estados não mais têm, teoricamente, o monopólio da força e dos meios de coerção. Dessa maneira, o espaço cibernético reduz a assimetria entre potências econômicas e militares, empresas privadas, grupos de indivíduos, e outros atores envolvidos nesse domínio, como será abordado mais adiante.

Assim sendo, o tema da cibersegurança tem sido pesquisado e debatido não só pela Academia, mas também por *thinktanks*, por governos e por entes privados, que são algumas das fontes utilizadas nesta pesquisa. É um assunto de interesse para inúmeros atores da sociedade internacional, pois ele pode influenciar fortemente o porvir, com alterações drásticas na maneira como funciona o mundo contemporâneo, tendo em vista a velocidade com que novas tecnologias disruptivas são desenvolvidas.

Sendo assim, o objetivo desse trabalho é compreender e estruturar o debate existente em torno do tema da segurança cibernética nas relações internacionais, analisando conceitos, argumentos e casos importantes para o tema, a fim de responder o seguinte questionamento: como a maior presença da segurança cibernética nas agendas dos Estados impacta a política internacional?

Para tanto, no presente artigo, primeiramente, se apresentará uma breve contextualização sobre a segurança cibernética; posteriormente, se discutirá o conceito de ciberespaço e serão apresentados os atores envolvidos; em seguida, serão apresentadas as discussões em torno do porquê da ocorrência do *cyberwarfare* e do poder cibernético, além dos desafios encontrados nessa seara; na última parte, se apresentará um breve histórico sobre alguns casos concretos de ataques paradigmáticos ocorridos no ciberespaço, e consequências para o desenvolvimento mais recente do tema.

1.1 Método e teoria

Segundo Teixeira (2007), uma pesquisa que busca compreender determinado fenômeno por meio de sua descrição e de sua interpretação, buscando uma profunda compreensão do contexto em que a situação se insere, e utiliza diferentes fontes de dados, é caracterizada como qualitativa. E é o que se faz nesse trabalho, com a compreensão e análise das diversas variáveis envolvidas. Ademais, nesse trabalho, várias fontes foram utilizadas, como livros especializados no assunto, artigos

científicos, artigos jornalísticos, discursos de autoridades, atas de conferências internacionais, relatórios governamentais, de instituições não governamentais, de entes privados ou de instituições acadêmicas, entre outros.

Realizou-se uma revisão da literatura em relação ao tema da segurança cibernética, com base na diversa variedade de fontes, conforme mencionado. Assim, os dados obtidos foram analisados e, por vezes, comparados, sempre sob a égide do objetivo principal de entender o lugar e o impacto da segurança internacional nas relações internacionais.Quanto aos objetivos da pesquisa, ela pode ser caracterizada como uma pesquisa exploratória, pois, segundo Gerhardt e Silveira (2009, p. 35), essa modalidade de pesquisa tem como finalidade "proporcionar maior familiaridade com o problema em questão, com vistas a torná-lo mais explícito ou a construir hipóteses". Além disso, as autoras afirmam que é costumeiro que essas pesquisas envolvam levantamento bibliográfico, conforme é o caso presente. Assim, quanto aos procedimentos adotados, a pesquisa pode também ser classificada como uma pesquisa bibliográfica, segundo classificação das mesmas autoras.

Como embasamento teórico deste trabalho, utilizou-se, em grande medida a vertente teórica pós-moderna das Relações Internacionais, tal como a dos trabalhos de James Der Derian, em segurança internacional, por exemplo. Para ele, e para os pós-modernos, em geral, as teorias tradicionais da disciplina não estão aptas a acompanhar as transformações da política mundial, pois a aceleração de processos no tempo, superando barreiras físicas e fixas do espaço territorial, alterou a dinâmica do poder no sistema internacional (NOGUEIRA, J. P.; MESSARI, N., 2005). Segundo os mesmos autores (2005, p. 209), fazendo uso dessa perspectiva pós-moderna, "são as trocas simbólicas, e não as materiais, que sustentam os diferentes regimes de dominação, constituindo novas articulações de poder/conhecimento". Der Derian afirma que o mundo tem sido alterado pela velocidade do surgimento de novas tecnologias, de forma que essas "inovações tecnológicas aumentaram o alcance das técnicas de vigilância e a velocidade de deslocamento das capacidades estratégicas – a violência e a guerra" (NOGUEIRA, J. P.; MESSARI, N.; 2005, p. 210). Eles também afirmam que esse deslocamento de capacidades acontece em tempo real, o que torna o espaço territorial uma mera abstração, um espaço virtual. Essa situação não reduz a probabilidade de conflitos; ao contrário, uma redefinição das estratégias

de dominação e de violência criam um regime de poder nas relações internacionais (DER DERIAN, J.; 1990 *apud* NOGUEIRA, J. P.; MESSARI, N.; 2005). Assim sendo, tem-se a ideia da importância do ciberespaço e, consequentemente, da segurança cibernética, nas relações internacionais contemporâneas. Diferente de tudo o que as teorias clássicas propunham, o espaço cibernético traz uma nova dinâmica à política internacional, tanto na diplomacia quanto nas questões estratégicas e militares, conforme será visto na próxima seção.

2. Segurança cibernética

Tradicionalmente, até a última década do século XX, alguns temas específicos dominavam a agenda de segurança internacional. Tópicos como guerras interestatais e intraestatais, segurança ambiental e segurança humana figuravam entre eles. Recentemente, entretanto, na virada do século e no início do século XXI, um novo assunto se juntou aos anteriores: a cibersegurança[1] (c*ybersecurity*). Além disso, por sua conexão com a revolução tecnológica e informacional que ocorre na sociedade contemporânea desde o último quartel do século passado, cujas principais características são a velocidade de propagação e o progressivo menor custo das informações, o tema da cibersegurança necessita ser constantemente atualizado, pois as tecnologias disponíveis no âmbito desse tema se aprimoram e se alteram com frequência.

Em 2012, a Organização para a Cooperação e Desenvolvimento Econômico (OCDE), lançou o relatório *Cybersecurity Policy Making at a Turning Point.* No referido relatório (OCDE, 2012), a organização analisou as estratégias nacionais de cibersegurança de dez de seus membros e destacou dois pontos em comum em praticamente todas as avaliações feitas pelos governos desses países, os quais demonstram a importância do tema da cibersegurança na política contemporânea: (i) a Internet e as tecnologias da informação são essenciais para o desenvolvimento econômico e social e compõem uma infraestrutura vital; (ii) as ameaças cibernéticas estão evoluindo e aumentando em um rápido ritmo. Ideia semelhante expressou o ministro das Relações Exteriores da França, Jean-Yves Le Drian, por ocasião da 72ª

[1] '*The technical and human means to detect, diagnose, stop and deter unwanted cyber operations*'. (WILLETT, 2019).

Assembleia Geral das Nações Unidas, em setembro de 2017. Segundo ele, nos últimos anos, o ciberespaço se firmou como um novo campo de oportunidades econômicas e de transformações sociais. Entretanto, Le Drian chamou atenção para alguns pontos importantes que não podem ser ignorados, mostrando que apesar das diversas oportunidades disponibilizadas pela emergência das tecnologias do ciberespaço, há, também, alguns efeitos deletérios e alguns riscos a se observar:

> Le monde numérique fait aussi face à des vulnérabilités nouvelles; elles sont susceptibles de remettre en cause les principes d'ouverture et de liberté qui fondent le cyberespace; elles ont également des conséquences néfastes sur les opportunités économiques qu'offre la révolution numérique. En réalité, nous assistons à une prolifération des menaces dans le cyberespace: ce phénomène représente un défi fondamental et il n'en est qu'à ses débuts; il s'intensifiera au cours des prochaines années, cela ne fait guère de doutes.[2]

Demonstrando, também, a importância da segurança cibernética no mundo atual, Jean-Claude Juncker, presidente da Comissão Europeia, afirmou, durante seu discurso sobre o estado da União, em setembro de 2017, que "*les cyberattaques peuvent être plus dangereuses pour la stabilité des démocraties et des économies que les fusils et les chars*"[3]. Nye (2018), no mesmo sentido, destaca que, desde 2013, o Diretor de Inteligência Nacional dos Estados Unidos classifica os riscos de cibersegurança como a maior ameaça àquele país. Assim sendo, como também informou um relatório produzido pelo *International Institute for Strategic Studies* (IISS), o *Strategic Survey 2018: The Anual Assessment of Geopolitics*, a revolução que envolve as novas tecnologias de informação e comunicação está moldando todos os aspectos do *statecraft*[4], incluindo a diplomacia, as estratégias de inteligência e o uso da força.

Especificamente no setor financeiro, à guisa de exemplo, Boer e Vazquez (2017) mencionam alguns dados sobre estimativas de prejuízo de ciberataques,

---

[2] "O mundo digital enfrenta também novas vulnerabilidades, as quais são suscetíveis a colocar em questão os princípios de abertura e de liberdade que são base do ciberespaço; elas têm também consequências nefastas sobre as oportunidades econômicas oferecidas pela revolução digital. Na verdade, nós assistimos a uma proliferação das ameaças no ciberespaço: esse fenômeno representa um desafio fundamental e que está apenas em seu início; ele se intensificará durante os próximos anos, disso não há dúvida" (tradução do autor).

[3] Os ataques cibernéticos podem ser mais perigosos para a estabilidade das democracias e das economias do que fuzis e tanques (tradução do autor).

[4] Conforme o dicionário Oxford (2015, p. 1509): "*skill in managing state and politicalaffairs*."

mencionando uma pesquisa feita pelo Lloyd's of London, em julho de 2017, que calculou que um único ciberataque em escala global, naquele momento, teria capacidade de infligir danos na ordem de 121 bilhões de dólares. O *Global Risks Report* 2018, do Fórum Econômico Mundial, cita uma pesquisa feita pelo *Juniper Research*, que estimou que o custo do cibercrime para as empresas, entre 2017 e 2022, seria de 8 trilhões de dólares.

Dessa maneira, a importância da segurança cibernética para a política internacional hodierna cresce progressivamente, em uma rápida velocidade. Por essa razão, o estudo do tema da segurança no espaço cibernético, nas relações internacionais, é de extrema importância para a tomada de decisão dos diversos atores e para a política internacional contemporânea. Assim sendo, entender o que é o espaço cibernético é um importante ponto de partida.

2.1 Ciberespaço

Um dos aspectos que tornam única a cibersegurança em relação aos outros temas de segurança internacional é o ambiente onde ela acontece. Antes de se aprofundar nos temas específicos de cibersegurança, é importante compreender a definição pormenorizada desse ambiente, o ciberespaço. Em razão das diversas nuances que são encontradas no espaço cibernético e de sua estrutura completamente nova à civilização humana e à sociedade internacional, o conceito de ciberespaço ainda suscita grandes debates e pouco consenso.

O princípio da Internet, e, por consequência, do ciberespaço atual, deu-se na década de 1960, por pesquisadores do *Massachusetts Institute of Technology* (MIT), da Universidade de Stanford e da Universidade da Califórnia, financiados pela DARPA (Agência de Projetos e Pesquisas Avançadas do Departamento de Defesa dos Estados Unidos), que criaram a ARPANET, uma rede para comunicação entre computadores dessas universidades e, também, para o Departamento de Defesa (CLARKE; KNAKE, 2015). Conforme os mesmos autores, nas décadas seguintes redes foram sendo aperfeiçoadas, códigos estruturados e protocolos desenvolvidos, o que permitiu o maciço crescimento na rede e a criação da Internet como a conhecemos hoje. Em 1996, apenas cerca de 36 milhões de pessoas (cerca de 1% da população mundial naquele momento) utilizavam a Internet; em duas décadas, no

início de 2017, esse número chegava a 3,7 bilhões de usuários, ou seja, por volta da metade da população mundial. Com seu desenvolvimento, principalmente a partir da década de 1990, as atividades no ciberespaço foram tornando-se cada vez mais presentes nas interações econômicas, políticas e sociais. Essa interdependência trouxe desenvolvimento e oportunidades econômicas, mas, também, vulnerabilidades e insegurança (NYE, 2018).

Primeiramente, deve-se ter em mente que o termo ciberespaço surgiu no último quartel do século XX para designar um novo ambiente que surgia e que era fundamentalmente diferente do mundo físico (RATTRAY, 2009). Em um primeiro momento, a maioria das pessoas relaciona o conceito de ciberespaço diretamente com a Internet; entretanto, apesar de incluir a *World Wide Web*, o ciberespaço é muito mais complexo do que isso, pois "o ciberespaço está presente em todas as redes de computadores do mundo e em cada coisa a elas conectada, ou por elas controlada", chamando atenção, também, para as redes intranets, por exemplo, que são redes privadas, utilizadas em empresas específicas ou por órgãos governamentais (CLARKE; KNAKE, 2015, p. 60). Singer e Friedman (2014) destacam, também, o fato de que o ciberespaço não é um ambiente puramente virtual, mas também possui sua parte no mundo físico, já que ele engloba as máquinas que armazenam os dados, a infraestrutura que possibilita o fluxo desses dados e, até, as pessoas que estão por trás dos computadores e demais dispositivos conectados ao ciberespaço. Em relação a essa infraestrutura física, Willet (2019) cita, como exemplo, os cabos de fibra ótica e os satélites de comunicação, o que, segundo o autor, mostra que o mito de que o ciberespaço é um ambiente puramente virtual não se sustenta.

Kuehl (2009), após uma análise de diversos conceitos prévios, define o ciberespaço como um ambiente que reside em redes caracterizadas pelo uso da eletrônica e do eletromagnetismo para criar, armazenar, modificar, transferir e explorar informação por meio de redes interdependentes e interconectadas, utilizando tecnologias da informação e de comunicação. Ademais, o ciberespaço pode ser visto como um ambiente operacional onde os seres humanos atuam com o propósito de atingir objetivos específicos, não diferindo muito, nesse ponto, dos outros quatro domínios físicos relacionados aos estudos de defesa: terra, mar, ar e espaço sideral. (KUEHL, 2009). Ademais, o ciberespaço é, neste século, uma zona de guerra onde

diversas batalhas decisivas acontecerão (CLARKE; KNAKE, 2015). Analogia interessante foi feita por Rattray (2009, p. 256), que observou o quanto a geografia do espaço cibernético é mais mutável que a dos outros ambientes. Segundo ele, "mountains and oceans are hard to move, but portions of cyberspace can be turned on and off with the flick of a switch; they can be created or 'moved' by insertions of new coded instructions in a router or switch". Além disso, Nye (2012a, p. 164) afirma que "o domínio cibernético é único, pois é feito pelo homem, é recente e está sujeito a mudanças tecnológicas ainda mais rápidas do que outros domínios".

Analisando o ciberespaço e as relações internacionais, Nye (2012a, p.161) afirma que "o espaço cibernético não vai substituir o espaço geográfico nem abolir a soberania do Estado, mas, como os mercados das cidades nos tempos feudais, vai coexistir e complicar muito o conceito de Estado soberano [...] no século XXI". Ao fazer essa afirmação, o autor salienta o fato de que o ciberespaço proveu oportunidades e caminhos para diversos outros atores não estatais atuarem na política internacional. De toda maneira, Nye (2012a) afirma que os Estados continuarão a ser os atores dominantes nas relações internacionais, embora o "palco" esteja cada vez mais povoado e difícil de controlar, em virtude da difusão de poder que o ciberespaço propaga. Outro desafio para os Estados decorrente da emergência do ciberespaço é o relativo ao domínio que estes exerciam na seara informacional, pois seu monopólio de alguns tipos de informação foi enfraquecido em favor de indivíduos e de atores não estatais (IISS, 2018).

De toda maneira, os Estados também obtiveram algumas vantagens com a emergência do ciberespaço, tanto no âmbito doméstico de suas políticas quanto no âmbito da política internacional. Segundo o Strategic Survey 2018 do IISS,

> States have also benefited from vastly increased opportunities for intelligence collection and the (deniable) subversion of rival states, as well as (in the case of authoritarian states) much greater capabilities to exercise social control over their own populations.

Choucri (2012) enumera e define quais são os desafios que a emergência e a consolidação do ciberespaço geram nas relações internacionais contemporâneas, principalmente se comparados com a abordagem tradicional da disciplina. A autora divide esses desafios em sete categorias diferentes: a) Temporalidade: o ciberespaço

altera a noção convencional de tempo para uma de quase instantaneidade; b) Espaço geográfico: a atividade cibernética transcende as limitações da geografia e da localização física; c) Permeação: o espaço cibernético penetra fronteiras e jurisdições; d) Fluidez: o ciberespaço promove e sustenta mudanças persistentes e reconfigurações; e) Participação: reduz as barreiras para o ativismo e para a expressão política; f) Atribuição: encobre identidades dos atores e das conexões; *g) Accountability*: supera os mecanismos de responsabilização estabelecidos.

É importante, também, mencionar uma visão que alguns autores têm sobre o ciberespaço: aquela de que as tecnologias cibernéticas podem promover o estabelecimento de uma "sociedade civil global", em razão da interconectividade que o ciberespaço proporciona aos cidadãos do planeta (REARDON; CHOUCRI, 2012). Os autores salientam, também, no levantamento que fizeram de artigos sobre o tema publicados na primeira década do século XXI, que quase todos os autores pesquisados percebem o ciberespaço como uma ferramenta de empoderamento, tanto de indivíduos como de outras organizações não estatais. Isto será analisado de forma mais detalhada na próxima seção.

2.2 Atores

Em razão de um profundo enraizamento histórico, a guerra é vista como um conflito entre dois Estados soberanos; todavia, quando o referente é a segurança cibernética, os atores não estatais possuem substancial relevância (FERNANDES, 2012). Rattray (2009) afirma que o grande número de atores que possuem papel importante no ciberespaço é o elemento principal que o distingue dos outros âmbitos da política internacional. Além disso, o autor afirma que os Estados não têm a capacidade de controlar o ciberespaço na mesma medida em que eles podem controlar os ambientes terrestre, marítimo e aéreo.

Nye (2012a) divide os atores no espaço cibernético em três categorias distintas: (i) governos, (ii) organizações com redes altamente estruturadas e (iii) indivíduos e redes fracamente estruturadas. Segundo o autor, todas as três categorias possuem suas vantagens e suas vulnerabilidades. Os atores governamentais são os próprios Estados-nação; as organizações não governamentais com redes altamente estruturadas incluem as corporações transnacionais e os grupos terroristas

estruturados, por exemplo; e os indivíduos e redes fracamente estruturadas são grupos civis pequenos e sem rede de estruturação e os próprios cidadãos. Em razão de seu didatismo e do excelente resumo que dispõe, reproduz-se, a seguir, tabela da obra do autor (Nye, 2012a, p. 174):

Principais governos

[Recursos/potencialidades:]

1 Desenvolvimento e apoio de infraestrutura, educação e propriedade intelectual.
2 Coerção legal e física de indivíduos e intermediários localizados dentro das fronteiras.
3 Tamanho do mercado e controle do acesso – por exemplo, União Europeia, China, Estados Unidos.
4 Recursos para ataque e defesa cibernéticos: burocracia, orçamentos, agência de inteligência.
5 Provisão de bens públicos, como as regulações necessárias para o comércio.
6 Reputação para a legitimidade, benignidade e competência que produzem poder brando.

Principais vulnerabilidades: alta dependência de sistemas complexos facilmente danificáveis, instabilidade política, possível perda de reputação.

Organizações e redes altamente estruturadas

[Vantagens/potencialidades:]

1 Grandes orçamentos e recursos humanos, economias de escala.
2 Flexibilidade transnacional.
3 Controle de desenvolvimento de código e produto, geração de aplicativos.
4 Marcas e reputação.

Principais vulnerabilidades: perseguição legal, roubo de propriedade intelectual, danos a sistemas, possível perda de reputação (denúncias).

Indivíduos e redes fracamente estruturadas

[Vantagens/potencialidades:]

1. Baixo custo de investimento para a entrada.
2. Virtual anonimato e facilidade de saída.
3. Vulnerabilidade assimétrica em comparação aos governos e às grandes organizações.

Principais vulnerabilidades: coerção legal e ilegal por parte dos governos e das organizações, caso sejam apanhados.

Nocetti (2018) destaca a emergência de organizações "hacktivistas", totalmente inéditas na política internacional, como o *Anonymous* e o *WikiLeaks,*

cujos objetivos podem ser políticos, ideológicos ou culturais. Ademais, o autor chama a atenção para atores não estatais mais clássicos, que já existiam antes, mas utilizam a web como uma plataforma operacional, como os grupos terroristas que a utilizam para planejar operações e recrutar combatentes. É o caso, segundo um relatório do Diretor Nacional de Inteligência dos Estados Unidos para um comitê do Senado norte-americano chamado *Foreign Cyber Threats to the United States*, de 2017, da al-Qa'ida, Hizballah, HAMAS e do autoproclamado Estado Islâmico, que continuavam, naquele momento, a utilizar a Internet para coletar informações de inteligência, coordenar operações, arrecadar fundos, disseminar propaganda e incitar novas ações.

Conforme o mesmo autor, há, ainda, alguns atores do ciberespaço que podem atuar como *proxies*, o que seria uma forma de determinados atores atuarem "por procuração", para lograr objetivos de terceiros interessados que os contratassem com tal fim. Nocetti (2018, p. 21) enumera alguns exemplos de atores que se encaixam nessa categoria:

> Plusieurs types d'acteurs peuvent être rangés sous le terme de proxies: des individus isolés, comme des hacktivistes opérant seuls ou des hackers malveillants louant leurs services; des réseaux d'hacktivistes agissant pour des motifs politiques ou des cybercriminels motivés par le profit (l'espace postsoviétique disposant de nombreux réseaux cybercriminels); des sociétés militaires ou de sécurité privée[5].

Cabe-se distinguir, também, os ciberterroristas dos cibercriminosos. De acordo com Ragot (2015), estes possuem objetivo mormente econômico, ou seja, procuram o enriquecimento por meio de atividades criminais no espaço cibernético. Já no caso dos ciberterroristas, há questões políticas, sociais e ideológicas envolvidas, além de objetivos distintos. Como forma de entender o que é especificamente o ciberterrorismo, Singer e Friedman (2014, p. 294) informam:

> As defined by the FBI, (cyberterrorism is) a 'premeditated, politically motivated attack against information, computer systems, computer

[5] Diferentes tipos de atores podem ser classificados sob o conceito de *proxies*: os indivíduos, como os hacktivistas que operam isoladamente ou como os hackers maliciosos que alugam seus serviços; as redes hacktivistas, que atuam por motivação política, ou as redes de cibercriminosos, motivados pelo lucro (o território pós-soviético dispõe de inúmeras dessas redes cibercriminais); e as sociedades militares ou de segurança privada (tradução do autor).

> programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents.

Como se mostrou, são diversos os atores que possuem, ou podem possuir, atuação significativa no ciberespaço: Estados, indivíduos, grupos ativistas organizados, empresas privadas, criminosos, terroristas, são alguns exemplos. Assim, nota-se a variedade de características distintas que esse grupo tão heterogêneo de atores possui. De toda maneira, ao atuar no espaço cibernético, esses atores utilizam algumas ferramentas e estratégias para exercer uma espécie de poder, o poder cibernético, tema que será abordado a seguir.

2.3 *Cyberwarfare* e o poder cibernético

Uma das facetas em que se dividem os temas de segurança cibernética é o *cyberwarfare*, relacionado à maneira como se conduz ataques cibernéticos e os instrumentos utilizados nesse processo. Primeiramente, segue uma definição generalizada de ataquecibernético :

> [...] les cyberattaques sont caractérisées par une utilisation d'outils ou de technologies afin de perturber, saboter, intercepter, détruire ou encore modifier des données informatisées ou des systèmes électroniques ou matériels présents dans le cyberespace (RAGOT, 2015, p. 57-58)[6].

Embora seja uma definição de caráter mais geral, ela descreve bem as principais características e propriedades que distinguem um ataque cibernético, tendo como definidores principais os objetivos visados e o meio em que ele ocorre.

O conceito de *cyberwarfare* é intrinsecamente interligado com aquele do poder cibernético (c*yberpower*). Segundo Kuehl (2009), poder cibernético é a habilidade de usar o ciberespaço para tomar vantagens estratégicas e para influenciar instrumentos de poder e eventos nos outros ambientes operacionais. Esse é o poder que os atores têm ao atuar no espaço cibernético, sejam eles atores estatais ou não estatais. Para Zimet e Barry (2009), o poder cibernético militar (*military cyberpower*) é a aplicação dos recursos cibernéticos para lograr objetivos militares, incluindo missões de assistência humanitária, de estabilização, de transição e reconstrução e,

[6] Os ciberataques são caracterizados pela utilização de instrumentos ou tecnologias com a finalidade de perturbar, sabotar, interceptar, destruir ou, ainda, modificar dados digitais ou sistemas eletrônicos ou materiais presentes no ciberespaço (tradução do autor).

principalmente, de combate bélico efetivo. Além disso, conforme observou Rattray (2009), as operações militares, a atividade econômica e o tráfego de ideias pelos outros domínios (terra, mar, ar e espaço exterior) são cada vez mais dependentes do funcionamento eficiente do espaço cibernético, ou seja, a importância e a influência do poder cibernético nas questões de defesa são cada vez maiores. Entretanto, deve-se notar, também, a importância e a potencialidade da utilização, em conflitos militares, do ciberespaço em combinação com os outros domínios clássicos, para lograr objetivos e auferir benefícios concretos. Segundo Gartzke (2013, p.44),

> Deterring or even defending against cyberattack may prove difficult, as other have argued, but it will prove much harder still for an attacker to figure out how to benefit from internet aggression, unless cyberattacks occur in conjunction with attacks in other domains.

É importante destacar as diferenças entre as características da guerra cinética e da guerra cibernética. Nye Jr. (2012a) destaca que, enquanto no plano físico os governos possuem, teoricamente, o monopólio dos meios de coerção em larga escala, conhecem intimamente o terreno e os conflitos terminam pelo desgaste ou pela exaustão, já que os recursos bélicos e a mobilidade são dispendiosos, no mundo cibernético os atores são diversos, muitas vezes anônimos, além de praticamente inexistir a distância física e o custo de perpetrar ciberataques é ínfimo, principalmente comparado aos meios tradicionais. Nye (2012b) destaca, por exemplo, que é bem mais barato e rápido mover elétrons pelo globo do que mover grandes embarcações de guerra para uma distância longa. Ademais, diferentemente das armas e tanques que caracterizam frequentemente um conflito bélico, as "armas" cibernéticas possuem um impacto primeiramente no campo da informação, e, por isso, seus efeitos são de difícil mensuração (CHIVVIS; DION-SCHWARZ, 2017). Nesse mesmo sentido, Gartzke (2013) salienta que existe uma diferença entre perpetrar um ataque cibernético e em realmente garantir que esse ataque terá como resultado alguma alteração nas relações de poder. Segundo o autor,

> It is one thing for an opponent to interrupt a country's infrastructure, communications, or military coordination and planning. It is another to ensure that the damage inflicted translates into a lasting shift in the balance of national power or resolve. (GARTZKE, 2013, p. 43).

Bello e Aderbigbe (2015) enumeram alguns tópicos em que o *cyberwarfare* difere dos conflitos bélicos cinéticos. São os seguintes: (i) a Internet é vulnerável; (ii) alto retorno do investimento; (iii) dificuldade em termos de ciberdefesa; (iv) alto grau de anonimidade; (v) participação de atores não estatais; (vi) baixo custo de entrada; (vii) torna imprecisas as fronteiras tradicionais; (viii) presença substancial de *perception management*[7]; (ix) ausência de inteligência estratégica atualizada; e (x) dificuldade de prever um ataque cibernético e de avaliá-lo. Ademais, há o fato de que, em um conflito tradicional, o Estado que recebe um ataque sabe, ou tem recursos para saber, quem foi o perpetrador do ataque; contudo, no espaço cibernético, o fator da atribuição possui características distintas.

Howard A. Schmidt, no *Emerging Cyber Threats Report for 2009*, do *Georgia Tech Information Security Center* (GTISC), apontou outro importante aspecto da arena cibernética em conflitos: "*cyber warfare completely evens the playing field as developing nations and large nations with a formidable military presence can both launch equally damaging attacks over the Web*". Pode-se adicionar, também, os atores não estatais nessa equação, já que o *gap* de poder efetivo entre eles e os Estados diminui consideravelmente quando o assunto é conflito cibernético.

Mesmo que a ciberguerra não substitua a tradicional guerra cinética, o ciberespaço oferece possibilidades adicionais para as tomadas de decisões dos governantes, pois terão novos recursos em suas mãos, para usar isoladamente ou conjuntamente com os meios convencionais de guerra (BELLO; ADERBIGBE, 2015). Entre esses recursos que podem ser utilizados no ciberespaço, encontram-se a espionagem, a propaganda, a implantação de bombas lógicas[8], a modificação de dados, a manipulação de infraestruturas e os ataques DDoS[9] (Ataque Distribuído de Negação de Serviço – *Distributed Denial of Service).*

Nocetti (2018) fornece quatro exemplos de ações ofensivas no ciberespaço, cada qual com um objetivo e uma técnica específicos:

---

[7] Refere-se, basicamente, à manipulação e controle de informações que chegam à opinião pública.

[8]Bomba-lógica é "uma aplicação de software ou uma sequência de instruções que desligam um sistema ou rede e/ou apagam todos os dados ou softwares da rede". (CLARKE; KNAKE, 2015, p.224).

[9]Segundo Clarke e Knake (2015, p. 16), um ataque DDoS é "basicamente um dilúvio pré-programado de tráfego na Internet projetado para derrubar ou congestionar uma rede". São realizados por meio dos *botnet*, "uma rede robótica de computadores 'zumbis' controlados remotamente".

a) Por meio de ataques DDoS, que têm por objetivo paralisar os servidores que são alvos desses ataques. São os ataques que aconteceram na Estônia, em 2007, e na Geórgia, em 2008, por exemplo;

b) Por meio de um vírus que se dirige deliberadamente a uma infraestrutura específica, como aconteceu com as centrífugas de urânio iranianas, em 2010, alvos do *Stuxnet*.

c) Propagando vírus de diferentes tipos, com o objetivo de extorquir dados e/ou dinheiro (caso do cibercrime clássico) ou de sabotar e destruir. Segundo o autor, um exemplo é a utilização de *ransonware*[10], como o *NotPetya* e o *WannaCry*, que serão mencionados mais adiante;

d) Por último, por meio da ciberespionagem, como o roubo de dados, os quais podem ser referentes a dados de indivíduos, a informações políticas ou militares, a propriedade intelectual etc.

Um relatório do Senado da República Francesa sobre a cibersegurança na União Europeia, registrado em abril de 2018, define, também em quatro pontos, os objetivos buscados por meio de ataques cibernéticos: (i) espionagem; (ii) cibercriminalidade, que possui por objetivo final o roubo e a extorsão de dinheiro ou de dados; (iii) desestabilização, pelas mídias sociais e sites de informação; (iv) sabotagem cibernética, ou seja, um ataque no mundo digital com o objetivo de paralisar ou destruir infraestruturas do mundo físico.

Nota-se que um ponto de extrema importância foi citado nesse relatório: o de desestabilização, que está relacionado, pois, à guerra da informação. Em relação a esse tema, a Conferência de Segurança de Munique, em fevereiro de 2017, declarou que os ataques cibernéticos não visam apenas às infraestruturas ditas críticas, mas, também, desde algum tempo, ao sistema político ocidental e os valores sobre os quais esse sistema é fundado (democracia representativa, separação dos poderes, liberdade de expressão etc.), o que leva alguns autores a sugerirem que a democracia e seus atributos devem ser tratados como uma infraestrutura crítica frente aos ataques cibernéticos e às manipulações da Internet (MUNICH SECURITY REPORT 2017 *apud* NOCETTI, 2018). Nesse caso, os atores agressores utilizam a propaganda, a

[10] *"A type of malware thatrestrictsaccess to a target and demandspayment to return regular service* » (SINGER; FRIEDMAN, 2014, p. 298).

desinformação, a difusão de *fake news*, a manipulação de informação, entre outras táticas. Segundo o autor, um ciberataque originado de um Estado tem como objetivo principal a produção de incerteza política, mais até do que os resultados destrutivos imediatos. Reproduz-se, a seguir, uma tabela que exemplifica as relações entre agressores e vítimas no ciberespaço, assim como possíveis estratégias e objetivos de ataques:

Tabela 1: Relações entre agressores e vítimas no ciberespaço

Tipos de agressores e de vítimas no ciberespaço		**Agressor**	
		Estado	**Ator Privado**
Vítimas	**Estado**	Um Estado ataca as infraestruturas de um outro Estado (ex.: Stuxnet).	Atores não estatais (grupos militantes ou "hackers patrióticos") atacam as redes de um Estado (ex.: Estônia, Geórgia).
	Ator privado	Um Estado ataca as redes privadas de outro Estado com fins estratégicos ou comerciais (ex.: Saudi Aramco, Sony Pictures).	Troca de hostilidades entre atores não estatais (ex.: ataques de grupos afiliados ao Anonymous contra o grupo Estado Islâmico).

Fonte: Nocetti, 2018, p. 18. (Tradução do autor).

Definidos os pontos que caracterizam a segurança cibernética, o conceito de ciberespaço, os atores envolvidos e suas relações, assim como algumas formas de ataques cibernéticos, é imperativo analisar quais são os principais desafios que os sujeitos envolvidos nessa seara enfrentam, já que o tema da segurança cibernética é relativamente novo na história da humanidade e das relações entre nações, fazendo com que alguns desses desafios sejam inéditos para a gestão governamental, por exemplo.

3 Desafios

3.1 O problema da atribuição

O problema da atribuição é, provavelmente, o principal em relação aos ataques na arena cibernética, pois a dificuldade para se atribuir um ataque a algum ator em específico dificulta qualquer retaliação contra o mesmo (SINGER; FRIEDMAN, 2014), o que impede o exercício pleno do direito de legítima defesa (NOCETTI, 2018). Segundo Singer e Friedman (2014), um exemplo é quando hackers enviam alguns tipos de *malware*[11] que controlam e fazem uso do computador da vítima sem que ela perceba, incorporando sua máquina pessoal em uma *botnet*[12], uma rede secreta de dispositivos interligados que pode atingir proporções extraordinárias, principalmente ao realizar ataques DDoS. Essa tática é utilizada quando há a intenção de esconder a identidade de quem está por trás dos ataques. Os autores avançam, e destacam que três características dessa capacidade de capturar e utilizar outros computadores são de fundamental importância. A primeira é de que não há limites geográficos para as *botnets*. Segundo, a de que o proprietário de um computador invadido geralmente não tem ideia de que sua máquina está sendo utilizada remotamente por alguém por causa de motivos questionáveis ou antiéticos. A terceira característica é que, na melhor das hipóteses, uma análise detalhada e minuciosa de um ataque perpetrado levará, normalmente, apenas ao computador do qual foi lançado o ataque, mas não a quem comandou essas máquinas de forma remota.

Com essas características em vista, tem-se que a atribuição formal de ataques cibernéticos é uma atitude rara, que depende menos de uma certeza técnica do que da vontade política de transmitir uma mensagem ou aviso a outro país (NOCETTI, 2018). Além disso, Gartzke (2013, p. 46) destaca que "*attackers are much more likely to strike if they are unlikely to be targeted in return*". Dessa maneira, a atribuição e a identificação do autor de ataques no espaço cibernético configuram

[11]Conforme Singer e Friedman (2014), *malware is a « malicious or malevolent software, including viruses, worms, and Trojans, that is programmed to attack, disrupt and/or compromise other computers and networks* ».

[12] Clarke e Knake (2015) definem *botnet* como "uma rede de computadores forçada a operar sob comandos de um usuário remoto não autorizado, geralmente sem o conhecimento de seu dono ou operador".

uma característica importante das atividades que acontecem nesse ambiente, influenciando tanto os perpetradores dos ataques quanto as potenciais vítimas, assim como retaliações e potenciais escaladas de tensão.

Esse problema da atribuição pode levar aos casos em que ataques são perpetrados contra um determinado Estado, por outro ente estatal, o qual nega seu envolvimento e atribui os ataques a *hackers* ativistas, da sociedade civil, conhecidos também como "cibercidadãos" (*netizens*) (FERNANDES, 2012). Um termo interessante utilizado para definir essa situação é o de "hacktivismo". O termo (*hacktivism*, originalmente) é definido por Singer e Friedman (2014, p. 77) como "the ideia of promoting or resisting some kind of political or societal change through nonviolent but often legally questionable cyber means of protest". Conforme os mesmos autores, o hacktivistas podem variar de indivíduos atuando isoladamente a organizações descentralizadas como o *Anonymous* e, também, organizações mais bem organizadas. Chivvis e Dion-Schwarz (2017) exemplificam essa situação citando a Rússia. Segundo os autores, suspeita-se que o governo russo faz uso constante de terceiros para desenvolver suas *cyber weapons* e para conduzir seus ataques, ou seja, os ataques originados de dentro do território russo podem, ou não, ser de iniciativa do Kremlin, o que dificulta fortemente um esforço de retaliação. É o caso do que aconteceu durante a *"Estonian Cyberwar*" e a atividade dos "hackers patrióticos" russos, temas que serão abordados mais à frente.

3.2 Vulnerabilidades

Outro desafio de extrema importância para a segurança cibernética de um Estado é a vulnerabilidade. Nye (2010) afirma que "depending on complex cybersystems for support of military and economic activities creates new vulnerabilities in large states that can be exploited by nonstate actors". Substancialmente expostas a essas vulnerabilidades estão as infraestruturas críticas. O *USA Patriot Act*, de 2001, aprovado após o ataque às torres do *World Trade Center*, definiu o conceito de infraestrutura crítica como

> […] systems and assets, whether physical or virtual, so vital do the United States that the incapacity or destruction of such systems and assets would

> have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

Willett (2019) dá o exemplo de infraestruturas críticas nacionais que têm sido objeto de ataques cibernéticos, como instituições financeiras, indústrias petrolíferas, instalações de energia nuclear, rede de energia elétrica e a estrutura de comunicação.

Quanto maior a dependência dessas infraestruturas em relação ao espaço cibernético, maior essa vulnerabilidade. Segundo o *Strategic Survey 2018* (IISS, 2018), as vulnerabilidades estão intrinsicamente ligadas ao "paradoxo da conectividade" (*connectivity paradox*), onde os Estados mais avançados tecnologicamente e dependentes das redes são, ao mesmo tempo, os mais vulneráveis a ataques cibernéticos.

McCarthy, Burrow, Dion e Pacheco (2009, p. 545) parafraseiam o 2003 *National Strategy to Secure Cyberspace*, dos Estados Unidos, dizendo que o ciberespaço é "the nervous system of the Nation's critical infrastructures, the control system of our country and the global economy". Segundo os autores, os Estados Unidos, por exemplo, são fortemente dependentes dessas infraestruturas críticas geridas no ciberespaço, e, por isso, um ataque cibernético contra essas infraestruturas causaria enormes danos, com impactos na segurança pública (por exemplo, um ataque nos sistemas de controle de uma barragem pode fazer com que ela se rompa e inunde cidades); na segurança nacional (como um ataque que torne acessível dados das agências de inteligência americanas ou informações militares); e segurança econômica (ataques que afetem a integridade do sistema financeiro). Muitos desses ataques a infraestruturas críticas são realizados com a implantação de bombas lógicas, que são colocadas em falhas dos sistemas e ficam aguardando para serem ativadas em tempos de tensão ou conflito (CLARKE; KNAKE, 2015). Isso é particularmente problemático, pois há dificuldade para se descobrir essas bombas lógicas: o tempo médio para descobri-las pode variar, por exemplo, entre 146 dias nos Estados Unidos e mais de 400 dias na União Europeia, o que retarda qualquer ação a respeito e permite que danos sejam imputados durante esse tempo. Ademais, as bombas lógicas possuem também a finalidade de servir como instrumento de aviso, pensadas para desencorajar, pelo medo de retaliação danosa, Estados a tomarem atitudes hostis. (IISS, 2018).

Clarke e Knake (2015) chamam a atenção para a vulnerabilidade norte-americana em sua rede elétrica, citando a informatização dos sistemas de controle das empresas desse setor a partir da década de 1990. Eles citam o exemplo de quão simples é autodestruir geradores elétricos por meio de comandos eletrônicos, pois, por meio de invasão das redes onde estão conectadas essas máquinas, os *hackers* podem fazer com que a rotação desses geradores seja excessiva, a ponto de destruir as pás de suas turbinas. Além disso, Gartzke (2013) afirma que as forças militares dos Estados Unidos se tornaram crescentemente dependentes de novas tecnologias para dominar o campo de batalha, embora, paradoxalmente, tenham se tornado mais vulneráveis e propensas a sofrer, cada vez mais, incidentes envolvendo ataques cibernéticos.

3.3 Outros desafios

Outro importante desafio para a segurança cibernética é o elevado risco de escalada de tensões no ciberespaço, muitas vezes relacionadas ao problema de atribuição. Nesse âmbito, estratégias de contenção são particularmente importantes. Nocetti (2018) cita como exemplo de estratégia a atitude da administração Obama em face ao roubo de dados do banco norte-americano JP Morgan, em 2014, e do vazamento de mensagens da Casa Branca e do Departamento de Estado, em 2015. Ao invés de acusar diretamente Moscou pelos ataques, já que havia indícios de que ambos os ataques foram praticados por hackers russos, talvez apoiados pelo governo russo, o governo estadunidense se absteve de qualquer declaração pública e deixou para que a imprensa o fizesse, enviando um aviso ao governo russo por meio da mídia, em substituição a uma atribuição formal por parte do governo norte-americano.

Particularmente, para os Estados nacionais, uma nova realidade é imposta pelo ciberespaço no que concerne suas atividades de inteligência. Recentemente, o número de empresas privadas de segurança cibernética tem crescido, muitas delas especialistas em recuperação e análise de programas espiões. Dessa maneira, elas tornam o conteúdo de suas pesquisas público e o transmitem na mídia, promovendo o acesso de qualquer cidadão ao conhecimento sobre as ferramentas de espionagem cibernética que os Estados têm, atualmente, a sua disposição. Nota-se a diferença do

que ocorria quando da Guerra Fria, quando as operações de espionagem dos Estados eram, na grande maioria das vezes, secretas. (NOCETTI, 2018).

Essa maior transparência e acessibilidade a fatos e dados relacionados à segurança cibernética é responsável pela divulgação e pela consequente análise de vários casos de conflitos cibernéticos, nas suas mais diversas formas. Dessa maneira, alguns casos são paradigmáticos para o estudo da segurança cibernética, por causa de suas características ou do contexto espacial e temporal em que ocorreram.

4 Histórico de casos paradigmáticos

Cavelty (2010) destaca a intervenção da Organização do Tratado do Atlântico Norte (OTAN) na então Iugoslávia, em 1999, como a primeira vez em que foram utilizados, de forma substantiva e constante, instrumentos de guerra de informação em combate, como propagadas, campanhas de desinformação pela mídia (segundo a autora, um importante aspecto dos instrumentos cibernéticos utilizados durante conflitos), ataques DDoS, ataques a websites iugoslavos e, possivelmente, a invasão das contas bancárias do líder iugoslavo Slobodan Milosevic pelas forças armadas estadunidenses. Por essa razão, o conflito ficou conhecido como a primeira guerra lutada no ciberespaço (CAVELTY, 2010).

Desde então, o espaço cibernético tem sido cada vez mais utilizado pelos atores envolvidos em uma contenda. Clarke e Knake (2015) citam alguns exemplos importantes ocorridos no segundo lustro da década de 2000. Em 2007, houve um ataque aéreo surpresa israelense contra uma suposta instalação nuclear na Síria. A despeito da defesa antiaérea síria, os caças israelenses adentraram no território do país vizinho sem maiores problemas; posteriormente, descobriu-se que Israel havia invadido o sistema de defesa sírio e inserido informações falsas. No mesmo ano, a Estônia foi vítima de um generalizado ataque DDoS, em um ataque atribuído a "hackers nacionalistas" russos, em razão de uma querela que envolvia a remoção de uma estátua que homenageava o Exército Vermelho, instalada durante o período da União Soviética. Rid (2012) afirma que o ataque partiu de cerca de 85.000 computadores infectados e durou três semanas. Os ataques tiraram do ar os websites de todos os ministérios do governo estoniano, os serviços online de dois grandes

bancos e até, em um momento, desativaram o servidor dos e-mails dos parlamentares. Alguns altos oficiais estonianos rapidamente acusaram a Rússia de estar por trás dos ataques, mas os especialistas técnicos tanto da Comissão Europeia quanto da OTAN não conseguiram evidências críveis de participação do Kremlin nos ataques (HERZOG, 2013). Além disso, o governo russo negou qualquer tipo de envolvimento nos ataques e os atribui a "hackers patrióticos", que teriam, segundo o governo, agido sem qualquer suporte governamental russo (SINGER; FRIEDMAN, 2014).

Em 2008, durante o conflito entre a Geórgia e a Rússia, que se unira às províncias separatistas Ossétia do Sul e Abecásia, um novo ataque cibernético generalizado foi dirigido à República da Geórgia. Novamente, o governo russo alegou que esses ciberataques eram uma atitude popular e que estavam fora do controle do Kremlin, mesmo que investigações tenham mostrado, posteriormente, que os sites usados para lançar os ataques eram conectados ao aparato de inteligência russa (MARKOFF, 2008). O autor chama a atenção, também, para o fato de os ataques cibernéticos contra a Geórgia terem sido praticamente concomitantes aos ataques da Força Aérea russa, já que um dos objetivos do ataque era fazer com que os georgianos não soubessem o que estava acontecendo naquele momento. Assim sendo, mostra-se mais um exemplo de como o espaço cibernético serve de instrumento importante no apoio a ataques cinéticos convencionais.

Já em 2010, ocorreu um dos ataques mais paradigmáticos envolvendo estratégias de ciberguerra. Naquele ano, uma instalação nuclear iraniana foi vítima de um ataque com o vírus Stuxnet, por alguns definido como "the first world's digital weapon" (ZETTER, 2014). Naquela ocasião, ficou claro que ataques cibernéticos podem ter efeitos consideráveis no mundo físico (NYE, 2012b). O Stuxnet foi criado, primeiramente, para sabotar sistemas de controle industriais utilizados em usinas energéticas e em gasodutos (FALLIERE; MURCHU; CHIEN, 2011). Em 2010, inspetores da Agência Internacional de Energia Atômica (AIEA) notaram que várias centrífugas de enriquecimento de urânio da planta de Natanz, no Irã, estavam quebrando. No final daquele ano, técnicos contratados pelo governo iraniano descobriram que o motivo do mau funcionamento dessas centrífugas era um vírus que estava presente em seu sistema, o qual fazia com que as centrífugas girassem

mais rápido do que a sua capacidade, consequentemente, quebrando-as (KUSHNER, 2013). Os sistemas da instalação nuclear iraniana de Natanz foram contaminados por esse vírus, o Stuxnet, provavelmente por meio de um dispositivo USB que foi conectado a algum computador pertencente à rede interna daquela instalação, e foi se reproduzindo e se espalhando pelo sistema. Ainda que o Irã não tenha revelado os números, é estimado que cerca de 984 centrífugas de enriquecimento de urânio foram inutilizadas, o que causou uma redução de 30% na produtividade do local (BROAD; MARKOFF; SANGER, 2011). Mesmo que nenhuma das partes tenha confirmado, acredita-se largamente que o ciberataque às instalações nucleares iranianas foi planejado e executado por meio de uma parceria entre os Estados Unidos e Israel (SANGER, 2012). Nocetti (2018) afirma que a operação do Stuxnet foi uma empreitada com um custo alto, pois vinha sendo planejada desde 2006, e representou um nível inédito de sofisticação técnica e de precisão operacional. Nye (2012b) cita, após o incidente com as centrífugas iranianas, que o Secretário de Defesa dos Estados Unidos naquele momento, Leon Panetta, advertiu os americanos do perigo de um "*cyber Pearl Harbor*" em um futuro próximo, pois, a partir da ocasião do Stuxnet, vários observadores afirmaram que esse era o prenúncio de uma nova forma de *warfare*. Contudo, o autor destaca que um "*cyber 9/11*" é bem mais provável do que um "*cyber Pearl Harbor*", já que este deixa implícito um ataque de um ator estatal, enquanto aquele se refere a atos catastróficos perpetrados por ator não estatal, uma forma de ciberterrorismo, que, segundo ele, é bem mais provável de acontecer.

Esses casos mencionados figuram massivamente na literatura como definidores do que é a cibersegurança hodiernamente, pois eles mostraram o que se é capaz de fazer através do espaço cibernético, como é importante o problema da atribuição e da defesa e a quantidade elevada de atores que podem participar dessas atividades. Entretanto, ataques cibernéticos não cessaram de ocorrer desde os casos citados. Nocetti (2018) afirma que, desde o verão de 2016, as ameaças cibernéticas entraram em uma fase de proliferação, de forma que novos casos têm surgido com frequência.

Um exemplo dessas ameaças de notável importância são os ataques envolvendo os *ransomwares* WannaCry e NotPetya, de intensidade até então inédita e que ocorreram em um espaço de dois meses, em 2017 (NOCETTI, 2018). O

primeiro, o WannaCry, em maio de 2017, atingiu mais de 300.000 computadores, em 150 países, e tinha como alvos principais algumas empresas, mas, também, certas infraestruturas críticas de alguns países (como o sistema de saúde britânico, as redes internas da polícia chinesa e os sistemas de transporte da Alemanha), com o prejuízo avaliado entre 4 e 8 bilhões de dólares (GREENBERG, 2018). Esse vírus explorava uma falha de segurança da Microsoft e bloqueava o acesso do proprietário dos computadores a seus respectivos sistemas, exigindo, assim, um resgate em bitcoins para devolver o acesso.

Poucas semanas depois, ocorreu o ataque com o NotPetya. Com o conflito entre a Rússia e a Ucrânia, iniciado efetivamente em 2014, a Ucrânia tornou-se um campo de testes para as táticas de ciberguerra da Rússia. Em 2015 e 2016, um grupo de hackers conhecido como *Sandworm* começou a detonar bombas lógicas em computadores tanto de organizações governamentais como de companhias privadas, destruindo vários *terabytes* de dados. Contudo, o ataque mais devastador do grupo foi em junho de 2017, com o lançamento do NotPetya. Esse malware se propagava de forma extremamente rápida e inédita e, diferentemente dos outros *ransomwares*, seu objetivo era basicamente destrutivo. Ainda que exigisse o pagamento de resgaste nos computadores contaminados, qualquer pagamento era inútil, pois a máquina já estava inutilizada, já que o vírus as danificava de modo irreversível. Lançado na Ucrânia e tendo como alvo principal esse país, rapidamente se propagou por computadores de todo o planeta, em questão de horas. Afetou gigantes multinacionais como a dinamarquesa A. P Moller-Maersk, a francesa Saint-Gobain e a filial europeia da norte-americana FedEx, a TNT Express, em todos esses casos infligindo prejuízos da ordem de centenas de milhões de dólares. Até mesmo a estatal russa Rosneft foi atingida. (GREENBERG, 2018). Em fevereiro de 2018, os países da aliança *Five Eyes*[13] atribuíram, publicamente, o ataque NotPetya à Rússia (NOCETTI, 2018).

[13]Aliança relacionada à inteligência que envolve cinco países anglófonos: Estados Unidos, Reino Unido, Nova Zelândia, Austrália e Canadá.

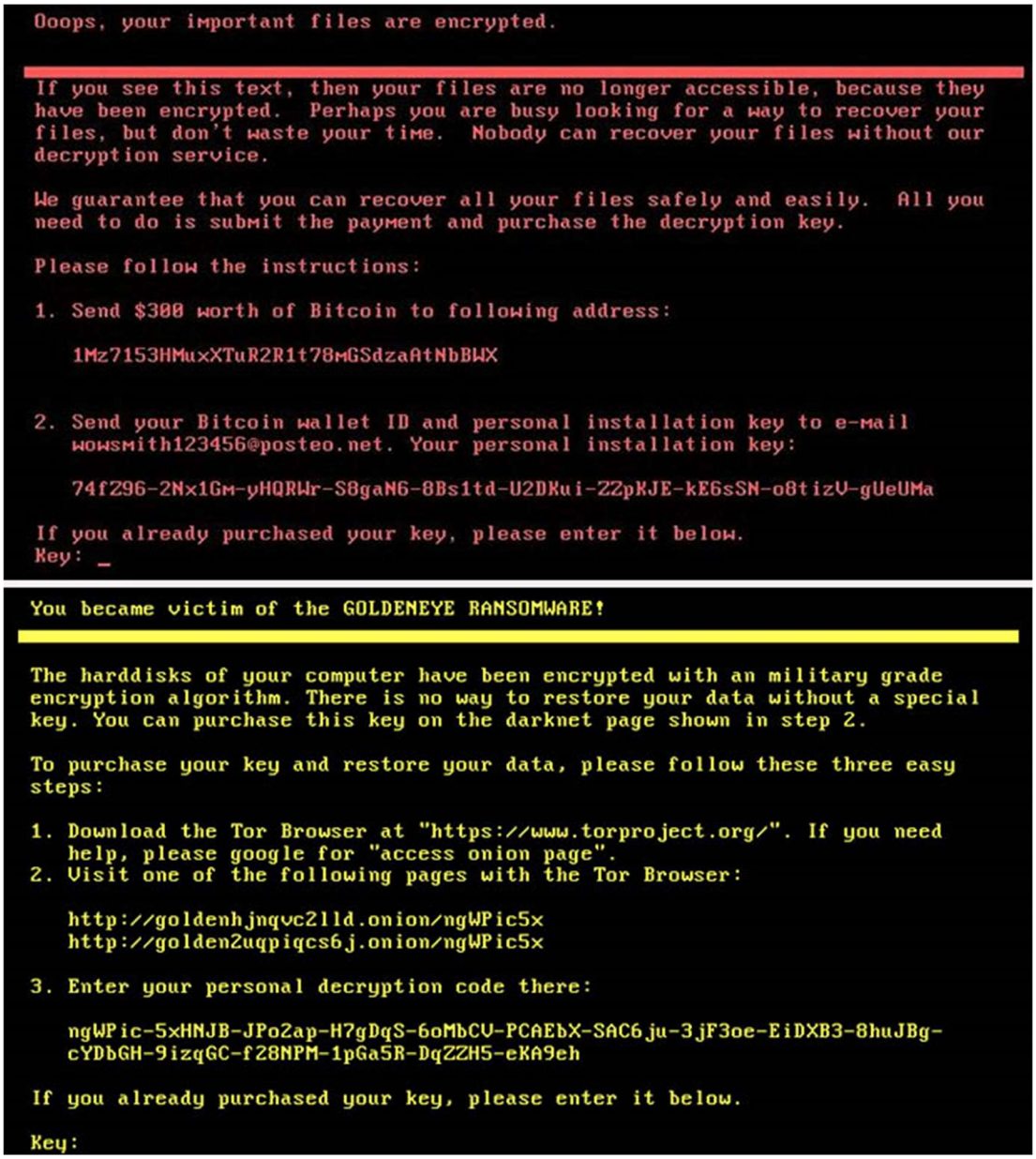

Figura 1: Telas de computadores infectados por *ransomwares*. Na tela superior, máquina infectada pelo NotPetya; na tela inferior, computador infectado pelo PetyaGoldeneye (Fonte: Symantec e Malwarebytes apud Rohr, 2017).

Recentemente, tem-se verificado, também, a realização de crimes cibernéticos, como o roubo de dados, para manipular informações e opiniões de indivíduos com vistas a influenciar resultados de eleições em alguns países. Geers e Kostyuk (2018) informam que, pouco antes das eleições de *midterm* nos Estados Unidos, em novembro de 2018, foi detectado por pesquisadores um incremento

expressivo na presença de *malwares* em treze específicos *swing states*[14], se comparados com os outros estados da federação. Eles afirmam que, com esse *malwares*, os hackers podem furtar, negar ou alterar qualquer tipo de informação digital, podendo ajudar, assim, determinados políticos a vencerem mais facilmente os pleitos eleitorais. O objetivo desses ataques era influenciar nas eleições que estavam prestes a acontecer, por meio do roubo de dados pessoais por esses malwares, o que possibilitaria, por meio dessas invasões, determinar o que o usuário da Internet verá e terá acesso, como a quais tipos de narrativas, e direcionar informações, como *fake news*, por exemplo, para os indivíduos vulneráveis a acreditar nessas informações.

Atribui-se também à Rússia uma interferência sistemática no ciberespaço durante as eleições presidenciais norte-americanas de 2016. Em uma das invasões ocorridas durante esse pleito presidencial, observou-se como um terceiro Estado poderia tirar vantagem da dificuldade de atribuição de ataques no ciberespaço em benefício próprio. É o caso de uma invasão nos servidores da Convenção Nacional do Partido Democrata, atribuída, na época, a um suposto hacker romeno, nomeado Guccifer 2.0; contudo, descobriu-se posteriormente se tratar de uma operação de *false flag*[15], como uma tentativa de encobrir a participação direta da Rússia no ataque (NOCETTI, 2018), que foi feita por meio de um grupo de hackers ligados ao Kremlin, chamado *Fancy Bear* (GREENBERG, 2018). A interferência russa também é alegada durante o processo de campanha eleitoral com uma estratégia focada em uma exploração habilidosa das mídias sociais. O *Strategic Survey 2018* (IISS) esclarece as bases e como funcionava o processo por trás dessa interferência:

> Russians purporting to be US citizens opened large numbers of fake social-media accounts, predominantly on Facebook and Twitter. These accounts were used to put out messages focusing on divisive social issues which were then amplified by bots (software applications that perform simple repetitive tasks at a much higher rate than humans can). This created the impression of a trending national debate on particular issues that could include anything from immigration and race relations to the behaviors of individual candidates, which US politicians then felt compelled to address and the traditional media to cover, thereby creating yet further amplification.

[14] Segundo o dicionário Oxford: "*(in an election for president in the US) a state where none of the candidates can be certain of getting the most support*".
[15] Segundo o dicionário Oxford: "*A political or military act orchestrated in such a way that it appears to have been carried out by a party that is not in fact responsible*".

Nota-se, então, uma estratégia relativamente bem estruturada, com processos definidos, utilizada por Estados nacionais para interferir em assuntos domésticos de outro Estado, com interesses velados e sem nenhuma confirmação pública do que foi feito.

O mesmo documento ainda destaca que, dias antes das eleições, hackers russos tentaram danificar o sistema de votação americano, enviando e-mails infectados com malwares para computadores dos oficiais eleitorais. Conforme o relatório, os objetivos russos eram, inicialmente, tentar gerar danos de imagem à candidata democrata, Hillary Clinton, e gerar desconfiança na opinião pública em relação ao processo político norte-americano. Posteriormente, trabalharam para promover a candidatura do candidato republicano, Donald Trump.

Este tipo de ataque cibernético é conhecido como guerra de informação, a qual ocorre em grande medida no ciberespaço. Nocetti (2018) cita como outro exemplo o que ocorreu na sequência dos ataques químicos de Duma, na Síria, em abril de 2018, pelas forças leais ao governo de Bashar Al-Assad. De acordo com o autor, depois desse ataque, a Rússia, aliada do regime, empregou uma estratégia baseada na difusão de informações que desorientassem a opinião pública ocidental e dividissem seus líderes.

Uma simples análise desses diversos eventos apresentados, ocorridos nos primeiros vinte anos do século XXI, demonstra a grande capacidade que os ataques cibernéticos têm para auxiliar os agressores a atingir seus objetivos e, também, para impor graves prejuízos às vítimas. Além da capacidade, fica notável a variedade de abordagens diferentes que podem acontecer, assim como a diversidade dos tipos de ataques que podem ser perpetrados. É importante destacar, também, que os conflitos citados são os conhecidos até o momento, e que isso não é uma fotografia fixa e imutável. O desenvolvimento de novas tecnologias propicia a elaboração de ataques com características inéditas, provavelmente inimagináveis no momento presente, vista a velocidade e a capacidade de evolução tecnológica da sociedade atual.

5 Conclusão

Analisando essa influência do ciberespaço na política internacional, chegou-se a diversas conclusões de como a segurança internacional tem impactado as relações internacionais. Embora haja uma profícua discussão em torno do conceito de ciberespaço, conforme foi apresentado nesse trabalho, um fato é consensual entre as diversas ideias apresentadas: é inequívoca e indubitável a importância, a influência e a omnipresença das tecnologias relacionadas ao espaço cibernético no cotidiano da civilização humana desde o início do século XXI. Como visto anteriormente, essa situação proporciona muitas oportunidades, com enorme potencial para o desenvolvimento econômico, social e político das nações; contudo, traz consigo, também, diversos desafios, os quais devem ser observados constantemente pelos atores envolvidos.

Como oportunidades, tem-se a minimização do custo do transporte, a relativização e a permeabilidade das fronteiras, a multiplicação da velocidade de transmissão de dados e a ampliação da capacidade e das ferramentas de gestão. Contudo, conforme dito, essa maior dependência do espaço cibernético trouxe, também, enormes desafios, destacando-se as acentuadas vulnerabilidades. Como afirmado ao longo deste artigo, há um paradoxo em que os países que mais se beneficiam das redes cibernéticas são, também, os mais vulneráveis a ataques nesse domínio. E é nessas vulnerabilidades que os governos nacionais têm que trabalhar, prioritariamente, quando o assunto é a segurança cibernética.

Mesmo que o conceito de espaço cibernético abarque diversos tópicos, porquanto não são consensuais na literatura, não há dúvidas de que esse é um novo campo de ocorrência de conflitos. Conflitos estes que podem ser interestatais, como os clássicos, mas, também, entre Estados e atores não governamentais, entre empresas privadas e grupos ativistas, entre outras combinações, dada a diversidade de atores presentes no ciberespaço. Atores estes que representam um grupo heterogêneo, englobando os indivíduos, os governos nacionais, organizações governamentais, organizações não governamentais, empresas privadas, grupos ativistas, criminosos e terroristas, para citar alguns.

Além dessa diversidade, é importante salientar a força comparativa que cada um possui, situação inédita nas relações internacionais, que, tradicionalmente, funda-

se, primordialmente, nos Estados. No espaço cibernético, estes não têm um poder relativo tão maior que os outros atores.

O tema da segurança cibernética é relativamente novo nos estudos das Relações Internacionais; mas isso não mitiga sua importância atual. Cada vez mais, em virtude das amostras de ataques disruptivos, como, mais recentemente, foi o caso do NotPetya, que demonstrou a capacidade de desarranjo que um único ataque pode causar, e os casos de guerras de informação, concebidas no espaço cibernético, a sociedade internacional tem se voltado para seu estudo. Vários Estados estão colocando em funcionamento suas próprias estratégias de cibersegurança, com pesados investimentos. Além disso, há mesmo casos de concertação multilateral no tema, como se tem visto em diversas declarações de conferências e cúpulas pelo mundo. Mais uma vez, isso é prova da importância da segurança cibernética para a política internacional contemporânea.

Espera-se que, em um futuro próximo, grandes iniciativas multilaterais ocorram em relação a esse tema. Como uma área potencialmente conflitiva, essa concertação entre os Estados não pode demorar a acontecer. Sendo assim, com o intuito de assessorar e influenciar a tomada de decisão de líderes por todo o mundo, a produção acadêmica e especializada no tema da segurança cibernética não pode parar; faz-se imperativo que ela avance cada vez mais nas discussões e na proposição de novas ideias.

REFERÊNCIAS BIBLIOGRÁFICAS

BELLO, O. A.; ADERBIGBE, F. M. Cyberwar – The New Frontier of International Warfare. **International Journal of Sustainable Development Research**. Vol. 1, Nº 1, p. 1-6, 2015. Disponível em : <http://article.sciencepublishinggroup.com/pdf/10.11648.j.ijsdr.20150101.11.pdf>. Acessado em: 05 fev. 2019.

BOER, M.; VAZQUEZ, J. **Cyber Security & Financial Stability:** how cyber-attacks could materially impact the global financial system. Institute of International Finance, set. 2017. Disponível em : <https://www.iif.com/Publications/ID/228/Cyber-Security-Financial-Stability-How-Cyber-attacks-Could-Materially-Impact-the-Global-Financial-System>. Acessado em: 16 mar. 2019.

BROAD, W.; MARKOFF, J.; SANGER, D. **Israeli Test on Worm Called crucial in Iran Nuclear Delay**. New York: New York Times, 15 jan. 2011. Disponível em: <https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html>. Acessado em: 27 fev. 2019.

CAVELTY, M. D. Cyber-threats. In: CAVELTY, M. D.; MAUER, V. (Ed.). **The Routledge Handbook of Security Studies**. Abingdon: Routledge, 2010. Cap 16.

CHIVVIS, C. S.; DION-SCHWARZ, C. **Why It's So Hard to Stop a Cyberattack – and Even Harder to Fight Back**. RAND Corporation, 2017. Disponível em: <https://www.rand.org/blog/2017/03/why-its-so-hard-to-stop-a-cyberattack-and-even-harder.html>. Acessado em: 5 fev. 2019....

CHOUCRI, N. Cyberpolitics in International Relations. Cambridge: MIT Press, 2012.

CLAPPER, J.; LETTRE, M.; ROGERS, M. **Joint Statement for the Record to the Senate Armed Services Committee:** Foreign Cyber Threats to the United States. Office of the Director of National Intelligence, 2017. Disponível em : <https://www.dni.gov/index.php/newsroom/congressional-testimonies/congressional-testimonies-2017/item/1614-joint-statement-for-the-record-on-foreign-cyber-threats-to-the-u-s-to-the-sasc>. Acesso em: 17 mar. 2019.

CLARKE, R; KNAKE, R. **Guerra cibernética:** a próxima ameaça à segurança e o que fazer a respeito. Rio de Janeiro: Brasport, 2015. Tradução do livro "Cyber War: the next threat to national security and what to do about it". HarperCollins, 2010.

COMISSION DES AFFAIRES EUROPÉENES - SÉNAT FRANÇAISE. **Proposition de résolution au nom de la commission des affaires européennes, en application de l'article 73 quater du Règlement, pour une cybersécurité robuste en Europe** : La cybersécurité : un pilier robuste pour l'Europe numérique. 20 abr. 2018. Disponível em : <http://www.senat.fr/basile/visio.do?id=r8104801_7&idtable=r8105789_11|r8104919_7|r8104899_12|r8104950_3|r8104737_9|r8104801_7|r8104971_15|r8104997_12&_c=ciberespace&rch=gs&de=20180316&au=20190316&dp=1+an&radio=dp&aff=sep&tri=p&off=0&afd=ppr&afd=ppl&afd=pjl&afd=cvn&isFirst=true>. Acessado em: 14 mar. 2019.

DER DERIAN, J. **The (S)pace of International Relations: Simulation, Surveillance and Speed.** International Studies Quarterly, n. 34, p. 295-310, 1990.

ESTADOS UNIDOS DA AMÉRICA. **Uniting and Strenghtening America by Providing Appropriate Tool Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001**. Public Law 107-56 – Oct. 26, 2001. Disponível em : <https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf>. Acessado em: 2 mar. 2019.

FALLIERE, N.; MURCHU, L. O.; CHIEN, E. **W32 Stuxnet Dossier**. Version 1.4. Symantec Security Response, feb. 2011. Disponível em : <http://large.stanford.edu/courses/2011/ph241/grayson2/docs/w32_stuxnet_dossier.pdf>. Acessado em: 27 fev. 2019.

FERNANDES, José Pedro Teixeira. A ciberguerra como nova dimensão dos conflitos do século XXI. **Relações Internacionais**, Lisboa, n.33, p. 53-69, mar. 2012. Disponível em: <http://www.scielo.mec.pt/scielo.php?script=sci_arttext&pid=S1645-91992012000100005&lng=pt&nrm=iso>. Acessado em: 15nov. 2018.

GARTZKE, E. The Myth of Cyberwar: bringing war in cyberspace back down to Earth. **International Security**, Cambridge, Vol. 38, Nº 2 (Fall 2013), p. 41-73. Disponível em: <https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00136>. Acessado em: 15 nov. 2018.

GEERS, K.; KOSTYUK, N. **Hackers are using malware to find vulnerabilities in U.S. swing states**. The Washington Post, nov. 2018. Disponível em: <https://www.washingtonpost.com/news/monkey-cage/wp/2018/11/05/hackers-are-

using-malware-to-find-vulnerabilities-in-u-s-swing-states-expect-cyberattacks/?utm_term=.6f637240af92>. Acessado em 2 mar. 2019.

GEORGIA INSTITUTE OF TECHNOLOGY INFORMATION SECURITY CENTER. **Emerging Cyber Threats Report for 2009**: data, mobility and questions of responsibility will drive cyber threats in 2009 and beyond. Atlanta, 15 out. 2008. Disponível em :<https://smartech.gatech.edu/handle/1853/26301>. Acessado em: 30 out. 2018.

GERHARDT, T. T.; SILVEIRA, D. T. **Métodos de pesquisa**. Porto Alegre: Editora da UFRGS, 2009.

GREENBERG, A. **The Untold Story of NotPetya**, the Most Devastating Cyberattack in History. Wired website, ago. 2018. Disponível em: <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>. Acessado em: 2 mar. 2019.

HERZOG, S. Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. **Journal of Strategic Security**. Vol. 4, nº 2, p. 49-60, Summer 2011. Disponível em :<http://scholarcommons.usf.edu/jss/vol4/iss2/4>. Acessado em: 15 nov. 2018.

INTERNATIONAL INSTITUTE FOR STRATEGIC STUDIES. The Impact of the ICT Revolution on International Relations. In: **Strategic Survey 2018:** The Annual Assessment of Geopolitics. Nov. 2018. Disponível em : <https://www.iiss.org/publications/strategic-survey/strategic-survey-2018-the-annual-assessment-of-geopolitics/ss18-04-strategic-policy-issues-2>. Acessado em: 27 fev. 2019.

JUNCKER, Jean-Claude. **Discours sur l'état de l'Union**. Strasbourg, 13 set. 2017. Disponível em : <https://ec.europa.eu/commission/news/president-juncker-delivers-state-union-address-2017-2017-sep-13_fr>. Acessado em 2 mar. 2019.

KUEHL, D. T. From Cyberspace to Cyberpower: defining the problem. In: KRAMER, F. D.; STARR, S. H.; WENTZ, L. K. (Ed.). **Cyberpower and National Security**. 1st ed. National Defense University Press; Potomac Books, 2009. Cap. 2.

KUSHNER, D. **The Real Story of Stuxnet**. IEEE Spectrum 53, nº 3, 2013. Disponível em: <https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet>. Acessado em: 27 fev. 2019.

LE DRIAN, Jean-Yves. **Cybersécurité : le rôle et la responsabilité des acteurs privés dans le renforcement de la stabilité et de la sécurité internationale du cyberespace**. Intervention de M. Jean-Yves Le Drian, ministre de l'Europe et des affaires étrangères de la République française. 72ème Assemblée générale des Nations unies. New York, 18 set. 2017. Disponível em : <https://basedoc.diplomatie.gouv.fr/vues/Kiosque/FranceDiplomatie/kiosque.php?fichier=bafr2017-09-19.html#Chapitre2>. Acessado em: 14 mar. 2019.

MARKOFF, J. **Before the Gunfire, Cyberattacks**. New York: New York Times, 12 ago. 2008. Disponível em: <https://www.nytimes.com/2008/08/13/technology/13cyber.html>. Acessado em: 27 fev. 2019.

MCCARTHY, J. A.; BURROW, C.; DION, M.; PACHECO, O. Cyberpower and Critical Infrastructure Protection: A Critical Assessment of Federal Efforts. In: KRAMER, F. D.; STARR, S. H.; WENTZ, L. K. (Ed.). **Cyberpower and National Security**. 1st ed. National Defense University Press; Potomac Books, 2009. Cap. 23.

NOGUEIRA, J. P.; MESARI, N. **Teoria das Relações Internacionais:** correntes e debates. Rio de Janeiro: Elsevier, 2005.

MUNICH SECURITY CONFERENCE. **Munich Security Report**. Munich, 2017. Disponível em : <www.securityconference.de/en/discussion/munich-security-report>. Acessado em: 14 mar. 2019.

NOCETTI, J. Géopolitique de la cyber-conflictualité. **Politique étrangère,** vol. 83, nº 2, été 2018. Disponível em : <https://www.ifri.org/fr/publications/politique-etrangere/articles-de-politique-etrangere/geopolitique-de-cyber>. Acessado em: 01 mar. 2019.

NYE JR, J. S. **Cyber Power**. Havard Kennedy School – Belfer Center for Science and International Affairs, mai. 2010. Disponível em : <https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf>. Acessado em: 27 fev. 2019.

_____. **Cyber War and Peace**. 2012b. Disponível em : <https://www.belfercenter.org/publication/cyber-war-and-peace>. Acessado em: 17 mar. 2019.

_____. **Normative Restraints on Cyber Conflict**. Cambridge: Belfer Center for Science and International Affairs (Harvard Kennedy School), 2018. Disponível em: <https://www.belfercenter.org/publication/normative-restraints-cyber-conflict>. Acessado em: 26 fev. 2019.

_____. **O futuro do poder**. 1ª ed. Tradução de Magda Lopes. São Paulo: Benvirá, 2012a.

ORGANIZAÇÃO PARA A COOPERAÇÃO E O DESENVOLVIMENTO ECONÔMICO. **Cybersecurity Policy Making at a Turning Point**. 2012. Disponível em: <http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf>. Acessado em: 08 mar. 2019.

OXFORD Advanced Learner's Dictionary. 8th ed. New York: Oxford University Press, 2015, p. 1509.

OXFORD Dictionaries. Online. Disponível em: <https://en.oxforddictionaries.com/definition/us/false_flag>. Acessado em: 9 abr 2019.

RAGOT, S. **Cyberespace, relations internationales et pays émergents :** évolution ou révolution? 2015. 226 f. Dissertação (Mestrado em Ciência Política) – Université du Québec à Montréal. Montréal, 2015. Disponível em: <https://archipel.uqam.ca/8651/1/M14081.pdf>. Acessado em: 27 fev. 2019.

RATTRAY, G. J. An Environmental Approach to Understanding Cyberpower. In: KRAMER, F. D.; STARR, S. H.; WENTZ, L. K. (Ed.). **Cyberpower and National Security**. 1st ed. National Defense University Press; Potomac Books, 2009. Cap. 10.

REARDON, R.; CHOUCRI, N. **The Role of Cyberspace in International Relations:** A View of the Literature. Cambridge: MIT, 2012. Disponível em: <https://nchoucri.mit.edu/sites/default/files/documents/%5BReardon%2C%20Choucri%5D%202012%20The%20Role%20of%20Cyberspace%20in%20International%20Relations.pdf>. Acessado em: 15 nov. 2018.

RID, T. Think Again: Cyberwar. **Foreign Policy**, 2012. Disponível em: <https://foreignpolicy.com/2012/02/27/think-again-cyberwar/>. Acessado em: 25 fev. 2019.

ROHR, A. **'Petya' x WannaCry**: veja diferenças do novo ataque cibernético. G1 website, 27 jun. 2017. Disponível em: <http://g1.globo.com/tecnologia/blog/seguranca-

digital/post/petya-x-wannacry-veja-diferencas-do-novo-ataque-cibernetico.html>. Acessado em: 14 mar. 2019.

SANGER, D. E. **Obama Order Sped Up Wave of Cyberattacks Against Iran**. New York: New York Times, 1 jun. 2012. Disponível em : <https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html>.Acessado em: 27 fev. 2019.

SINGER, P. W.; FRIEDMAN, A. **Cybersecurity and Cyberwar:** what everyone needs to know. New York: Oxford University Press, 2014.

TEIXEIRA, E. **As Três Metodologias:** acadêmica, da ciência e de pesquisa. 4ª Ed. Petrópolis: EditoraVozes, 2007.

WILLETT, M. **Cyber instruments and international security**. The International Institute for Strategic Studies, 2019. Disponível em : <https://www.iiss.org/blogs/analysis/2019/03/cyber-instruments-and-international-security>. Acessado em: 13 mar. 2019.

WORLD ECONOMIC FORUM. **The Global Risks Report 2018** – 13th Edition. Genebra, 2018. Disponível em : <https://www.weforum.org/reports/the-global-risks-report-2018>. Acessado em: 27 fev. 2019.

ZETTER, K. **An unprecedented look at Stuxnet, the world's first digital weapon**. Wired website, 11 mar. 2014. Disponível em: <https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/>. Acessado em: 25 fev. 2019.

ZIMET, E.; BARRY, C, L. Military Service Overview. In: KRAMER, F. D.; STARR, S. H.; WENTZ, L. K. (Ed.). **Cyberpower and National Security**. 1st ed. National Defense University Press; Potomac Books, 2009. Cap. 12.